UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF 9 BIRCH LANE, DAMARISCOTTA, ME 04543, WHITE 2009 VOLKSWAGEN JETTA ME REG. 7445ZG, AND THE PERSON AND PERSONAL EFFECTS OF TREY KNOF	)	Case No. 2:23-mj-00115-KFW
	)	Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

I, Dale D. Wengler, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") currently assigned to the Augusta, Maine Resident Agency of the FBI's Boston Division. I have been employed as an FBI Special Agent for over eleven years. As an FBI Special Agent, I am authorized to conduct investigations of and to make arrests for federal criminal offenses. During my tenure with the FBI, I have investigated white-collar criminal matters and federal criminal offenses involving child pornography, civil rights, public corruption, and healthcare fraud. I have received training and gained experience in the investigation of computer-related crimes, including crimes involving children.

2. I submit this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a warrant authorizing the search of three locations more fully described in Attachment A and a subsequent search of any devices seized from these three locations, including the entire property located at 9 Birch Lane, Damariscotta, Maine 04543 ("Subject Premises"), the vehicle registered to Trey Knof ("Knof"), and the person of Knof as well as any personal effects in his actual possession for evidence, contraband, and instrumentalities concerning criminal violations of 18 U.S.C. §§ 2252A(a)(2)(A) and

(b)(1) (distribution of child pornography) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of child pornography) more fully described in Attachment B.

3. The facts set forth in this affidavit come from my direct involvement in this investigation, my training and experience, information obtained from other law enforcement personnel as well as information obtained through administrative subpoenas, interviews, and physical surveillance. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

PROBABLE CAUSE

A. Transfer of Suspected Child Sexual Abuse Material via Kik[1]

4. The FBI is conducting an investigation of suspected criminal violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of child pornography) involving Knof. This investigation arises out of Knof's use of the mobile application Kik to transfer suspected child sexual abuse material.

5. In August 2022, an online covert employee ("OCE")[2] with the FBI was conducting an ongoing covert investigation on Kik. Posing as an adult male with access

[1] Based on my training, experience, and investigation, I know that Kik is a free mobile application, designed for chatting and messaging, that is available for download on both the iOS App Store and the Google Play Store. After installing the application and creating a unique username, a Kik user can view, send, and receive texts, images, videos, and more. In addition to communicating one-on-one, Kik users can communicate in both public and private chat groups. Upon joining a particular group chat, a Kik user can view, message, and share content, including images and videos, with the entire group or any other user in the group.

[2] Based on my training, experience, and investigation, I know that the term "online covert employee" refers to an FBI employee, typically a Special Agent or a Task Force Officer,

to a minor female, namely his fictious 11-year-old daughter, the OCE joined a public chat group on Kik where information posted by other group members indicated that members of this group were interested in obtaining links to child pornography.[3]

6. On about August 24, 2022, a Kik user with the username georgey1345 initiated contact with the OCE, following which the OCE and georgey1345 exchanged the following messages:[4]

From:	**To:**	**Message:**
georgey1345	OCE	Do you trade links or anything?
OCE	georgey1345	I have a kid for play
OCE	georgey1345	Depends on if ur legit
OCE	georgey1345	I'm near Philly
georgey1345	OCE	I'm near Boston

Based on my training, experience, and investigation, I understand the OCE's use of a phrase "a kid for play" in this context to mean having custody or control over a child who is available to engage in sexually explicit conduct with an adult.

7. The OCE asked georgey1345 about playing "Irl," which I know to be a common slang abbreviation for the phrase "in real life," and georgey1345 responded by

who has received training and certification by the FBI to engage in online undercover activities.

[3] I have omitted the name of the Kik chat group and the OCE's Kik username in this affidavit to avoid compromising the FBI's broader ongoing covert investigation.

[4] The messages reproduced in this affidavit contain multiple typographical errors. These are errors that were contained in the original messages, and I have not corrected them.

sending two different Mega[5] links to the OCE, after which the OCE and georgey1345 continued sending the following messages to each other:

From:	To:	Message
OCE	georgey1345	Nice lol any of you? U play for real
georgey1345	OCE	Sadly no, I wish I could play
OCE	georgey1345	Lol it seems your legit with those links so lmk
OCE	georgey1345	I don't keep anything she's mostly no limits
OCE	georgey1345h	She's eleve n
georgey1345	OCE	You don't keep any videos of her?
OCE	georgey1345	No way bitch ex wife would find it and crush me
OCE	georgey1345	I film the guy playing and usually jerk off
georgey1345	OCE	Wish I had a kid lol and could do the same
OCE	georgey1345	Like I said those links make u legit so she's available
OCE	georgey1345	I think i gotta go through them I thought I saw young
georgey1345	OCE	The second link is young
georgey1345	OCE	The first link was teens
OCE	georgey1345	Ah I love yung but hard to find like infant and toddler

[5] Based on my training, experience, and investigation, I know that Mega provides cloud storage and file hosting services in an encrypted format through its website, https://mega.io, and its free mobile application, which is available for download on both the iOS App Store and the Google Play Store. After signing up for an account with a valid email address, a Mega user can designate one or more folders on their device, which Mega synchronizes with the user's account. As a result, that same folder with those same contents, including image and video files, can appear on both the user's device and their Mega account. A Mega user also can share folders with other people by sending links, which gives the recipients of links the ability to access the contents of those public folders, including any files placed in them.

Based on my training, experience, and investigation, I understand the OCE and georgey1345's use of the term "young" or "yung" in this context to mean child pornography.

8. After further discussion about the OCE's minor daughter, georgey1345 sent a third Mega link to the OCE, which also contained suspected child sexual abuse material.[6]

9. I have personally reviewed the contents of the second Mega link, which contained approximately 3.6 gigabytes of suspected child sexual abuse material, that georgey1345 sent to the OCE via Kik on about August 24, 2022, pursuant to which I learned the following facts:

a. Included among the suspected child sexual abuse material are several videos that depict minors, including babies and toddlers, engaging in sexually explicit conduct.

b. One such video is named "Baby Lexxa." This video, which is approximately one minute and fifty seconds in duration, depicts, among other things, a male who is putting a penis in a baby's mouth, a male who is attempting to penetrate a baby's anus, and a male who is masturbating and eventually ejaculates on a baby. The video concludes with the following text: "What a sexy little baby cunt! Maybe I'll shit on the bitch next time!"[7]

c. Another such video, which is approximately one minute and thirty-seven seconds in duration, depicts a baby that is being penetrated by a male's penis. The male then masturbates and ejaculates in the baby's face and mouth.

[6] Because it was blocked and removed, I have not personally reviewed the contents of the third Mega link that georgey1345 sent to the OCE via Kik on about August 24, 2022.
[7] A representative still image from this video is attached under seal as Exhibit A.

B. Identification of Knof and the Subject Premises

10. Additional investigation by the FBI established that the Kik user with the username georgey1345 was linked to the email address georgeysnow1345@yahoo.com, which was initially registered with Yahoo! on about August 17, 2022. The IP addresses affiliated with georgey1345's Kik account traced back to several different public wi-fi networks in and around Damariscotta, Maine. The FBI also learned that the recovery telephone number associated with the email address georgeysnow1345@yahoo.com was 207-248-7692, which was a TracPhone with no listed subscriber.

11. Further investigative efforts by the FBI established that the telephone number 207-248-7692 appeared to be associated with Knof. Based on my review of Knof's criminal history, I know that Knof is a registered sex offender with prior state convictions, including: dissemination of sexually explicit material of a minor, possession of sexually explicit material of a minor, gross sexual assault, sexual abuse of a minor, unlawful sexual touching, and violating release conditions.

12. I personally confirmed that Knof most recently spent approximately 441 days in state custody for dissemination of sexually explicit material of a minor and possession of sexually explicit material of a minor. I also personally confirmed that Knof was released from state custody on these charges on about August 12, 2022, which is approximately 5 days before the email address georgeysnow1345@yahoo.com was created and approximately 12 days before georgey1345 transferred the suspected child sexual abuse material to the OCE via Kik.

13. I also personally confirmed that Knof is currently serving a two-year term of state probation. In addition, I personally reviewed the state probation intake paperwork completed by Knof on about August 15, 2022, pursuant to which Knof gave

the telephone number 207-248-7692 as his current cell phone number. This is the same telephone number as the recovery number associated with the email address georgeysnow1345@yahoo.com.

14. Pursuant to my review of Knof's state probation file, I know that on about August 16, 2022, Knof told a state probation officer that he was temporarily residing at the Schooner Inn in Wiscasset, Maine. Based on my direct involvement in this investigation, I also know that the IP address associated with the creation of the email address georgeysnow1345@yahoo.com, which was linked to the Kik user with the username georgey1345, also traces back to the Schooner Inn in Wiscasset, Maine. In addition, I know that Knof subsequently moved to the Subject Premises and that Knof told a state probation officer that he currently lives at 9 Birch Lane, Damariscotta, Maine 04543.

15. Pursuant to my review of the reports associated with Knof's prior state offenses, I learned that in March 2021, Knof hid an Apple iPhone and a Samsung smartwatch in his bedroom closet, despite being under state bail conditions that prohibited him from possessing any Internet-capable devices. I also learned that Knof's then-roommate told law enforcement that Knof likely had another internet-capable device hidden somewhere, noting that an Android charger went missing from the kitchen after Knof left their shared residence. In addition, I learned that Knof also obtained and distributed suspected child sexual abuse materials to others via Kik in the past, including sending at least one Mega link where the recipient responded, "[t]eens not toddlers[.]"

16. On about February 15, 2023, I conducted surveillance in the area of the Subject Premises, which I observed to be comprised of both a mobile home and a small shed. I also observed a white Volkswagen Jetta with Maine license plate 7445ZG at the

Subject Premises. A query of this Maine license plate number showed the registered owner of this vehicle is Knof.

CHILD PORNOGRAPHY, DIGITAL DEVICES, AND THE INTERNET

17. Based on my training and experience and my discussions with other law enforcement personnel, I know the following:

a. Digital devices, such as computers, cellular telephones, tablets, and electronic storage media, and digital technology are the primary way in which individuals interested in child pornography interact with each other today. These devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. For example, digital cameras and cellular telephones save images and videos as digital files that can be directly transferred to a computer by connecting the digital camera or cellular telephone to the computer, using a cable or using wireless connections, such as "WiFi" or "Bluetooth." Images and videos also may be stored on a removable memory card within a particular digital device, such as a cellular telephone. Removable memory cards are often large enough to store thousands of high-resolution images and videos.

c. A device known as a modem allows one computer to connect to another computer through the use of telephone, cable, or wireless connection. Other digital devices, such as cellular telephones and tablets, may connect to one or more computers using wireless connections, such as "WiFi." Through wired or wireless connections, a digital device can contact literally millions of computers around the world. Child pornography therefore can be easily, inexpensively, and

relatively anonymously produced, distributed, received, and stored by anyone with access to one or more digital devices.

d. A digital device's ability to store images and videos in a digital format makes it an ideal repository for child pornography. Electronic storage media of various types, including computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer, can store thousands of high-resolution images and videos. It is extremely easy for an individual to take an image or a video with a digital camera or a cellular telephone, upload that image or video to a computer, and then copy it (or any other files on the computer) to any one of these electronic storage media. Some electronic storage media, such as "thumb," "jump," or "flash" drives, can easily be concealed and carried on an individual's person. Cellular telephones likewise are often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or cellular telephone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography typically can be found on the user's computer, cellular telephone, tablet, or electronic storage media.

g. A growing phenomenon related to cellular telephones, tablets, and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps, including Kik or Mega, consist of software downloaded onto digital devices that enable users to perform a variety of tasks–such as engaging in online chats or sharing digital files–using one's digital device. Individuals commonly use apps to access, store, distribute, and advertise child pornography, to interact directly with other like-minded individuals or with potential minor victims, and to access cloud-based storage services where child pornography may be stored for extended periods.

h. As is the case with most digital technology, communications exchanged by way of a digital device can be saved or stored on the device used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

INDIVIDUALS INTERESTED IN CHILD PORNOGRAPHY

18. Based on my training and experience and my discussions with other law enforcement personnel, I also know that there are certain characteristics common to individuals who are interested in child pornography, including the following:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexually explicit activity or in sexually suggestive poses, including in person or in media.

b. Such individuals may collect sexually explicit or sexually suggestive materials in a variety of media, including images, videos, or other visual media. Individuals who have a sexual interest in children often use these materials for their own sexual arousal and gratification. They also may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate desired sexual acts. In addition, they may retain their online communications with other like-minded individuals.

c. Such individuals typically store their child pornographic materials and related communications in a digital format in a relatively secure and private environment, such as their digital devices (*e.g.*, computer, cellular telephone, tablet, or electronic storage media). Such individuals commonly keep digital devices containing these illicit materials at the possessor's residence, including the house, garage, or shed, inside the possessor's vehicle, or on the possessor's person, which allows the possessor not only to keep these materials relatively secure and private, but also to keep them nearby and easily accessible.[8]

[8] Based on my training, experience, and investigation, I know that individuals interested in child pornography often use cellular telephones and tablets to create, circulate, and retain their child pornographic material and that people tend to keep their cellular telephones and tablets on their person or otherwise close to them, such as at their home, garage, shed, or inside their vehicle.

d. Some of these individuals may maintain material involving child pornography and related communications on their digital devices for extended periods. Others may access, view, and delete material involving child pornography on their digital devices on a cyclical basis.

19. Based on all the facts set forth here, there is probable cause to conclude that Knof shares certain characteristics common to individuals who are interested in child pornography. There also is probable cause to conclude that shortly after his most recent release from state custody for sex offenses involving children—including dissemination of sexually explicit material of a minor and possession of sexually explicit material of a minor—Knof, using the Kik username georgey1345, exchanged the previously described messages with the OCE and sent a Mega link containing suspected child abuse material to the OCE via Kik. Additionally, there is probable cause to conclude that evidence, contraband, and instrumentalities concerning criminal violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of child pornography) will be found at the Subject Premises, in Knof's vehicle, and on Knof's person.

DIGITAL DEVICES, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. As further described herein and in Attachment A, this application seeks permission to search for records and information that might be found at the Subject Premises, in Knof's vehicle, or on Knof's person, in whatever form they are found, pursuant to Rule 41(e)(2)(B). One form in which the records are likely to be found is digital data stored on one or more digital devices (*e.g.*, computers, cellular telephones, tablets, or electronic storage media). Some digital data may take the form of files, images, videos, communications, and other user-generated data. Other digital data may become

meaningful only upon further forensic analysis. Based on my training, experience, and communications with other law enforcement personnel, there is probable cause to conclude that digital data will be stored on any digital devices seized at the locations described in Attachment A because:

a. Digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Digital files downloaded to a digital device can be stored for extended periods at little or no cost.

b. Even when digital files have been deleted, they can be recovered months or even years later using forensic tools. This is because when a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Deleted files or remnants of deleted files may reside in free space or slack space—that is, in space on the device that is not currently being used by an active file—for extended periods before they are overwritten. In addition, a digital device's operating system also may keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic storage media—particularly internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information,

but users typically do not erase or delete this electronic evidence because special software is usually required to do so.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a digital device's temporary Internet directory or "cache." An Internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them from the digital device.

21. As further described in Attachment B, this application seeks permission to locate not only digital data on digital devices that might serve as direct evidence of the suspected criminal violations, but also to locate forensic evidence that establishes how any such devices were used, the purpose of the use, who used them, and when. Based on my training, experience, and communications with other law enforcement personnel, there is probable cause to conclude that forensic evidence will exist on any digital devices seized at the locations described in Attachment A because:

a. Data on digital devices (*e.g.*, computers, cellular telephones, tablets, or electronic storage media) can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that shows what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the

attachment of USB flash storage devices or other external storage media, and the dates and times the device was in use. Internal file systems can record information about the dates and times files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within digital devices can provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Such stored information (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and antivirus, spyware, and malware detection programs) also can indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of antivirus, spyware, and malware detection programs may indicate whether the device was remotely accessed, thus inculpating or exculpating the device's owner or primary user.

c. Further, data on digital devices can indicate how and when a device was accessed or used. For example, a device typically contains information that logs: user account session times and durations, activity associated with user accounts, electronic storage media that connected with the device, and the IP addresses through which the device accessed networks and the Internet. Such information allows investigators to understand the chronological context of access, use, and other relevant events relating to the crimes under investigation.

d. Moreover, some stored information may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the user.

e. Last, information stored within digital devices may provide relevant insight into the user's state of mind as it relates to the crimes under investigation. For example, such stored information may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

22. A person with appropriate familiarity with how digital devices work can, after examining this forensic evidence in its proper context, draw conclusions about how the devices were used, the purpose of their use, who used them, and when.

23. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on digital devices that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on computers, cellular

telephones, tablets, or electronic storage media is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

24. Further, in finding evidence of how devices were used, the purpose of their use, who used them, and when, sometimes it is necessary to establish that a particular thing is not present on a device. For example, the presence or absence of counter-forensic programs or antivirus programs (and associated data) may be relevant to establishing the user's intent.

25. Based on my training, experience, and communications with other law enforcement personnel, I know that when an individual uses the Internet to access, receive, and distribute child pornography, the individual's digital devices generally will serve both as an instrumentality for committing the crime and as a storage medium for evidence of the crime, including contraband. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device also is likely to be a storage medium for evidence of the criminal offense, including contraband. More specifically, a device used to commit these types of crimes may contain: data concerning how the device was used; data concerning what was sent or received, data concerning when materials were sent and received and by whom, data concerning how the criminal conduct occurred; records of Internet discussions about the criminal conduct; and other records that indicate the nature of the offense and the identity of the offender.

26. Based on my training, experience, and communications with other law enforcement personnel, I know that data can be stored on a variety of systems and storage devices, including computers, cellular telephones, tablets, gaming systems, external and

internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, SIM cards, memory cards, memory chips, other magnetic or optical media, and online and offsite storage servers maintained by corporations, including but not limited to, cloud storage and file hosting services. I also know that during the search of a place or a person where such devices are located, it is not always possible to search any located devices for a number of reasons, including:

a. Searching such devices is a highly technical process that requires specific expertise and specialized equipment. There are so many types of hardware and software in use today that it is impossible to bring all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it also may be necessary to consult with personnel who have specific expertise in the type of device, software, or operating system that is being searched;

b. Searching such devices requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Some hardware may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since digital data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the device from which the data will be extracted;

c. The volume of data stored on many such devices typically will be so large that it will be highly impractical to search for data during the execution of the physical search of different locations; and

d. Users can attempt to conceal data within devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Users also can attempt to conceal data by using encryption, which means that a password or other device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

27. Based on my training, experience, and communications with other law enforcement personnel, I know that searching digital devices for evidence, contraband, or instrumentalities of a crime often requires the seizure of all input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that law enforcement can accurately retrieve the device's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the digital devices vary widely in their compatibility with other hardware and software. Many devices require particular input/output devices in order to read the data on the system. It is important that law enforcement be able to properly

reconfigure the system as it now operates to accurately retrieve the stored data. In addition, law enforcement needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

b. To fully retrieve data from certain digital devices, such as a computer system, law enforcement also needs all magnetic storage devices, as well as the central processing unit (CPU).

28. Additionally, based on my training, experience, and communications with other law enforcement personnel, I know that routers, modems, and network equipment used to connect devices to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of a cybercrime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set

up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

29. Based on the foregoing, and consistent with Rule 41(e)(2)(B), this application seeks a warrant that also would permit seizing, imaging, or otherwise copying of digital devices (*e.g.*, computers, cellular telephone, tablets, or electronic storage media) that reasonably appear to contain some or all the items described in the warrant, and would authorize later review of the media, data, or other information consistent with the warrant. The later review may require techniques, including but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is an item described by the warrant.

30. Law enforcement intends to make and retain a full image copy of any seized media, so that a copy of the evidence, rather than the original evidence, can be examined. Law enforcement will retain both the original evidence and any copies of this evidence. This procedure will ensure that the original evidence remains intact.

CONCLUSION

31. Based on the forgoing, I respectfully request that the Court issue the proposed warrant, which authorizes law enforcement to search three locations, which are more fully described in Attachment A, and perform a search of any digital devices seized from these three locations, including the Subject Premises, Knof's vehicle, and Knof's person for evidence, contraband, and instrumentalities concerning criminal violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of child pornography) as more fully described in Attachment B.

32. Based on my training, experience, and communications with other law enforcement personnel, I know that the recovery of digital data by a forensic analyst takes significant time. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the locations specified. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Dale D. Wengler, Special Agent
Federal Bureau of Investigation

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedures

Date: May 02 2023

Judge's signature

City and state: Portland, Maine

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title